



PCT

 WELTORGANISATION FÜR GEISTIGES EIGENTUM

 Internationales Büro

 INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE

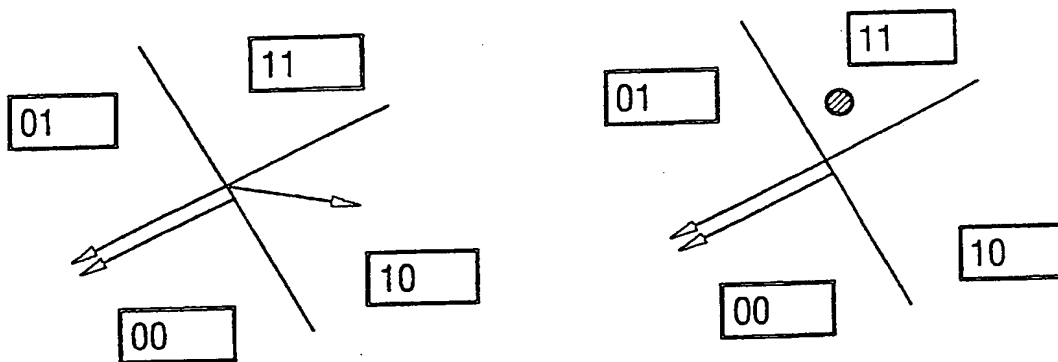
 INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation ⁷ : G06K 9/46, G07C 9/00	A1	(11) Internationale Veröffentlichungsnummer: WO 00/60533 (43) Internationales Veröffentlichungsdatum: 12. Oktober 2000 (12.10.00)
--	-----------	---

(21) Internationales Aktenzeichen: PCT/DE00/01020 (22) Internationales Anmeldedatum: 3. April 2000 (03.04.00) (30) Prioritätsdaten: 199 15 463.5 6. April 1999 (06.04.99) DE (71) Anmelder (für alle Bestimmungsstaaten ausser US): SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D-80333 München (DE). (72) Erfinder; und (75) Erfinder/Anmelder (nur für US): RAAF, Bernhard [DE/DE]; Maxhofstr. 62, D-81475 München (DE). (74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D-80506 München (DE).	(81) Bestimmungsstaaten: CN, HU, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Veröffentlicht <i>Mit internationalem Recherchenbericht. Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i> <div style="text-align: center; margin-top: 20px;"> <i>Transkription</i> </div>
--	---

(54) Title: METHOD AND DEVICE FOR USER AUTHENTICATION

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR NUTZER-AUTHENTIFIKATION



(57) Abstract

The invention relates to a method and a device for user authentication on the basis of a biometric complex of characteristics which is detected in the form of a surface pattern. From said surface pattern a plurality of characteristic elements are extracted, quantized positional and/or directional relations of said characteristic elements in relation to each other and/or to defined reference points or reference directions are determined, a number is assigned to each characteristic element and an identification number is calculated from said numbers.

(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren sowie eine Vorrichtung zur Nutzer-Authentifikation aufgrund eines als Flächenmuster erfaßten biometrischen Merkmalskomplexes, wobei aus dem Flächenmuster eine Mehrzahl von charakteristischen Merkmalselementen extrahiert wird, quantisierte Lage- und/oder Richtungsbeziehungen der Merkmalselemente zueinander und/oder zu vorbestimmten Bezugspunkten bzw. -richtungen ermittelt werden, jedem Merkmalselement eine Element-Zahl zugeschrieben wird und aus den Element-Zahlen eine Identifikations-Kennzeichnung berechnet wird.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidshan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Beschreibung

Verfahren und Vorrichtung zur Nutzer-Authentifikation

- 5 Die vorliegende Erfindung betrifft ein Verfahren und eine Vorrichtung zur Nutzer-Authentifikation, d.h. zur Prüfung der Zugangsberechtigung einer Person zu einem Objekt, System oder Dienst im allgemeinsten Sinne.
- 10 Die Prüfung der Zugangs- bzw. Zugriffsberechtigung zu verschiedenartigen Geräten, System und Diensten bzw. Leistungen gewinnt mit der explosionsartigen Verbreitung neuer Informations- und Kommunikationstechnologien immer mehr an Bedeutung und erfordert einerseits mit zunehmendem Nachdruck benutzer-
- 15 freundliche und andererseits hochgradig zuverlässige Lösungen. So sind die Grenzen der Nutzung von Geheimzahlen (PIN) und Paßworten in einem Umfeld, in dem praktisch jedermann eine Vielzahl von Zugangsberechtigungen zu verschiedenen Geräten und Systemen haben und täglich nachweisen muß und in
- 20 dem andererseits immer bessere Möglichkeiten für die Ausforschung derartiger Zugangsberechtigungen bestehen, erreicht. Daher gewinnt die Nutzer-Authentifikation aufgrund hochgradig individueller und unfälschbarer biometrischer Merkmale zunehmend an Bedeutung.
- 25 Auf solchen Merkmalen, wie etwa dem Papillarlinien- oder Retinamuster, beruhende Authentifikationsverfahren und -vorrichtungen sind bekannt und beispielsweise bei Zugangskontrollsystemen für bauliche Objekte oder bei Geldautomaten
- 30 auch bereits im praktischen Gebrauch. Sie beruhen grundsätzlich darauf, daß das individuelle Papillarlinien- oder Retinamuster eines berechtigten Nutzers im Zugangskontrollsystem gespeichert ist und ein Zugangsuchender seinen Fingerabdruck oder sein Netzhautmuster durch eine geeignete Erfassungsein-
- 35 richtung erfassen und mit den gespeicherten Mustern der Berechtigten vergleichen lassen muß. Durch zusätzliche Identifikatoren, beispielsweise Name, Personal- oder Kundennummer

oder PIN, erfolgt üblicherweise die Spezifikation eines einzigen potentiell Berechtigten, so daß nur das diesem Berechtigten zugeordnete Flächenmuster mit dem entsprechenden Flächenmuster des aktuell Zugangsuchenden verglichen werden
5 muß. Dies erleichtert und beschleunigt die Arbeit solcher Systeme erheblich, so daß zunehmend auch ihr Einsatz in Geräten des täglichen Bedarfs, bei denen eine Nutzer-Authentifikation erforderlich oder zweckmäßig ist, in Erwägung gezogen wird.

10

Die Benutzung eines Mobiltelefons ist bekanntlich nur nach Eingabe einer vierstelligen PIN möglich, die dem Nutzer bei Vertragsabschluß zugewiesen wird und auf der SIM-Karte gespeichert ist. Die Zugangsberechtigung zum Netz wird nach
15 jedem Einschalten des Mobiltelefons im Ergebnis eines Vergleichs der eingegebenen mit der gespeicherten PIN erteilt (oder verweigert). Im Interesse einer unkomplizierten Handhabung wird bei den gebräuchlichen Mobilfunksystemen keine Nutzer-Authentifikation bei jedem Systemzugriff (Anruf)
20 gefordert; dies hat aber bekanntlich den Nachteil, daß ein eingeschaltetes Mobiltelefon ohne weiteres mißbräuchlich benutzt werden kann.

Zudem hat die übliche - und in den Systemprotokollen festgelegte - PIN-Authentifikation die oben erwähnten grundsätzlichen Nachteile, insbesondere den Nachteil der Unbequemlichkeit des Einprägens und immer wiederkehrenden Handhabens einer zunehmenden Anzahl von PINs im täglichen Leben. In diesem Zusammenhang ist auch darauf hinzuweisen, daß die PIN im
25 Grunde reine Software darstellt, die grundsätzlich auch mit ausschließlich softwaremäßigen Mitteln kopiert bzw. simuliert werden kann, während eine Nutzer-Authentifikation aufgrund biometrischer Merkmale in dem Bezug zum Körper des Zugreifenden stets eine "Hardware"-Zuordnung beinhaltet. Überdies gibt
30 die Unbequemlichkeit einer PIN- oder Paßworteingabe durch eine Mehrzahl von Tastenbetätigungen immer wieder Anlaß zu Umgehungslösungen. So kann bei manchen Mobilfunkdiensten der

Nutzer die PIN-Authentifikation (auf eigenes Risiko) gänzlich deaktivieren.

Schließlich ist darauf hinzuweisen, daß speziell bei Mobiltelefonen ein eindeutiger Trend zu einer Handhabungserleichterung durch weitgehenden Verzicht auf Tasteneingaben besteht. Bei vielen neueren Geräten sind zumindest die alphanumerischen Tasten bei der Standard-Nutzung abgedeckt, und eine Zifferneingabe wird mehr und mehr auf Sonderfälle beschränkt. Auch tastaturlose "Easyphones" sind im Gespräch. Diesem Trend steht die Nutzer-Authentifikation durch Tasteneingabe einer PIN entgegen.

Angesichts der ins Auge springenden Vorteile einer biometrischen Authentifikation, insbesondere der Unvergeßbarkeit und des überaus hohen Aufwands für ein Kopieren bzw. Fälschen eines biometrischen Merkmalskomplexes, ist daher deren Einsatz auch zur Zugriffssteuerung von Mobiltelefonen vorgeschlagen worden.

20

Gemäß einer durch die Anmelderin früher vorgeschlagenen Lösung kann aus dem Flächenmuster eines Fingerabdrucks aufgrund eines vorbestimmten Codierungsalgorithmus eine PIN berechnet werden. Diese wird dann auf übliche Weise mit der auf der SIM-Karte gespeicherten PIN verglichen. In diesem Rahmen wurde auch vorgeschlagen, durch Nutzung verschiedener Berechtigungsalgorithmen aus den Fingerabdrücken mehrerer autorisierter Nutzer ein und dieselbe PIN zu berechnen und damit allen autorisierten Personen die Benutzung des Mobiltelefons zu ermöglichen. Dieser Lösungsvorschlag ist systemkonform zum GSM-Standard und kombiniert erhöhte Benutzerfreundlichkeit mit größerer Sicherheit, erfordert aber die Speicherung und Verarbeitung sehr großer Datenmengen in der Größenordnung von 1 GB und ist daher derzeit nur bedingt praktisch realisierbar.

35

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung zur Nutzer-Authentifikation anzugeben, das mit relativ geringem Speicher- und Verarbeitungsaufwand auskommt.

5

Diese Aufgabe wird durch ein Verfahren mit den Merkmalen des Anspruchs 1 bzw. eine Vorrichtung mit den Merkmalen des Anspruchs 8 gelöst.

- 10 Die Erfindung schließt den wesentlichen Gedanken ein, nach der bildverarbeitenden Auswertung eines gesamten, als Flächenmuster vorliegenden biometrischen Merkmalskomplexes eine Extraktion charakteristischer Elemente vorzunehmen und die Lage- bzw. Richtungsbeziehungen der ausgewählten Elemente
15 zueinander bzw. zu vorbestimmten Bezugspunkten bzw. -richtungen nach einem für eine digitale Verarbeitung geeigneten Schema zu bestimmen und zu codieren. Aus der so ermittelten, relativ kleinen Anzahl von Zahlen wird dann eine Identifikations-Kennzeichnung (PIN oder Paßwort o.ä.) bestimmt, die
20 einem Vergleich mit einer abgespeicherten Identifikations-Kennzeichnung unterzogen wird.

- Als charakteristische Elemente eines individuellen Flächenmusters werden bevorzugt Linienenden und -verzweigungen eines
25 in dem erfaßten Flächenmuster enthaltenen Linienmusters, speziell der Papillarlinien eines Fingerabdrucks, hinsichtlich ihrer Lage- bzw. Richtungsbeziehungen ausgewertet. Daneben können aber auch andere charakteristische Merkmale, wie beim Fingerabdruck etwa die sogenannten "weißen Linien", Einschlüsse oder Delta-Bereiche, durch Zuweisung eines binären
30 Codes unter - ebenfalls in einer entsprechenden Binärzahl enthaltenen - Positions- und/oder Richtungsangabe registriert werden. Für andere als Flächenmuster darstellbare biometrische Merkmalskomplexe lassen sich andere charakteristische
35 Elemente bzw. Punkte finden, die eine Auswertung mit verringertem Speicherbedarf ermöglichen, so beispielsweise für ein Sprachfrequenz- bzw. Voice-Diagramm lokale Minima und Maxima.

Da die erfindungsgemäße Lösung bewußt von einem Punkt-für-Punkt-Vergleich des auszuwertenden biometrischen Musters abgeht und ihre Vorteile hinsichtlich des Speicherplatzbedarfs insbesondere bei einer relativ groben Positions- bzw. Richtungszuordnung der charakteristischen Merkmale zum Tragen kommen, ist durch Wahl eines geeigneten fehlerkorrigierenden Berechnungsalgorithmus in zweckmäßiger Weise dafür zu sorgen, daß Erkennungs- und Zuordnungsfehler in begrenztem Umfang ohne Auswirkung auf die Bestimmung der Identifikations-Kennzeichnung bleiben. Nur beispielhaft sei hier auf bekannte fehlerkorrigierende Codes wie die Convolutional Codes, Reed-Solomon Codes oder Block-Codes hingewiesen. Hierbei sind mit ähnlicher Zielstellung etablierte, dem Fachmann bekannte Codierungsverfahren aus der Nachrichtentechnik analog einsetzbar.

Umfaßt die Berechnungsvorschrift vordefinierte "Verwürfelungen", läßt sich aus einem gegebenen, individuell stabilen Merkmalskomplex gleichwohl eine beliebige Identifikations-Kennzeichnung erzeugen. Umgekehrt ermöglicht die Verfügbarkeit mehrerer, auf die individuellen Merkmalskomplexe der einzelnen berechtigten Nutzer spezifisch adaptierter Berechnungsvorschriften die Ableitung ein und derselben Identifikations-Kennzeichnung aus verschiedenen biometrischen Merkmalskomplexen, so daß bei einer solchen Ausführung eine Authentifikation mehrerer Nutzer auf der Basis einer einzigen gespeicherten Identifikations-Kennzeichnung möglich ist.

In einer Ausführung, in der die Identifikations-Kennzeichnung ausschließlich aus dem biometrischen Merkmalskomplex abgeleitet werden soll, also eine parallele oder hilfsweise Tasteneingabe nicht vorgesehen ist, muß die Kennzeichnung (PIN o.ä.) auch dem berechtigten Nutzer gar nicht bekannt sein, sondern es ist die Speicherung im zu schützenden Gerät bzw. System oder, genauer gesagt, dem zugeordneten Zugriffskontrollsystem ausreichend. Diese Variante ist besonders

benutzerfreundlich, es kann aber infolge des Verzichts auf die Möglichkeit einer Tasteneingabe der Kennzeichnung im Einzelfall (etwa bei stark verschmutzten Fingern) Zugriffsprobleme geben. Ist mit Blick auf dieses Problem das System zu einer Tasteneingabe parallel zur Erfassung des biometrischen Merkmalskomplexes ausgebildet, besteht vorzugsweise die Möglichkeit eines Wechsels der Kennzeichnung, wozu ein oder mehrere Reserve-Berechnungsalgorithmen zur Verfügung stehen. Da mit jedem Verfahren für ein und dasselbe Papillarlinienmuster eine andere Kennzeichnung berechnet wird, steht eine der Anzahl der zusätzlichen Berechnungsverfahren entsprechende Zahl von Reserve-Kennzeichnungen bereit.

Durch Einbeziehung einer Fehlergrenz-Information bei der Gewinnung der Element-Zahlen kann zum Ausdruck gebracht werden, um welchen Betrag die Lage oder Richtung eines Merkmals verschoben werden müßte, damit eine andere Element-Zahl (speziell Binärzahl bzw. Bitfolge) entsteht. Auf dieser Grundlage läßt sich in der nachfolgenden Codierung eine sogenannte "soft-decision" ausführen.

Vorteile und Zweckmäßigkeiten der Erfindung ergeben sich im übrigen aus den Unteransprüchen sowie der nachfolgenden Erläuterung bevorzugter Ausführungsformen anhand der Figuren. Von diesen zeigen

- Fig. 1 ein Papillarlinienmuster mit verschiedenen charakteristischen Merkmalselementen,
- Fig. 2 zwei Beispiele für die binäre Codierung der Richtung bzw. Lage eines Merkmalselements relativ zu einem Bezugssystem,
- Fig. 3 eine Illustration zur Erläuterung der Auswertung einer vorbestimmten Merkmals-Gesamtheit eines Fingerabdrucks zur Bestimmung einer PIN und
- Fig. 4 ein schematisches Funktions-Blockschaltbild einer Vorrichtung zur Nutzer-Authentifikation bei einem Mobiltelefon.

Fig. 1 zeigt als Beispiel für ein einen biometrischen Merkmalskomplex darstellendes Flächenmuster das Papillarlinienmuster eines Fingerabdrucks. Die Ziffern bezeichnen verschiedene charakteristische Merkmale, nämlich Ziffer 1 das Zentrum, Ziffer 2 eine Gabelung, Ziffer 3 weiße Linien, Ziffer 4 einen sogenannten Einschluß, Ziffer 5 ein sogenanntes rechtes Delta, Ziffer 6 ein (abruptes) Linienende und Ziffer 7 ein sogenanntes linkes Delta. Die bevorzugte Ausführung des vorgeschlagenen Verfahrens beruht auf der Binärcodierung der Position und/oder Orientierung derartiger Merkmalselemente und der nachfolgenden Umsetzung des n-Tupels aus den n erhaltenen Binärzahlen in eine PIN.

Fig. 2 soll verdeutlichen, wie die Codierung der den Merkmalen zugehörigen Lage- bzw. Richtungsinformation grundsätzlich erfolgen kann. Im linken Teil von Fig. 2 ist symbolisch ein Pfeil als Merkmal bzw. Flächenmusterelement in einem kartesischen Koordinatensystem gezeigt, dem eine (als Doppelpfeil dargestellte) Referenzrichtung zugeordnet ist. Wie in der Figur dargestellt, wird die Richtung des Merkmals in der Binärdarstellung durch zwei Bit repräsentiert, wobei eine Differenzierung nach dem Quadranten erfolgt, in den der Pfeil weist. Beim gezeigten Beispiel hätte die Richtung des Pfeils die Binärdarstellung "10".

Im rechten Teil von Fig. 2 ist skizziert, wie die binäre Repräsentation der Lage eines Merkmals (ausgefüllter Kreis) in dem gleichen kartesischen Koordinatensystem mit gespeicherter Referenzrichtung erfolgt. Der hier gezeigte ausgefüllte Kreis hat die binäre Lagekennzeichnung "11".

Allgemein gesagt, können eine oder mehrere Positionen bzw. Richtungen gespeichert werden, wobei im einfachsten Fall ein Bit (1 oder 0) zu einer - sehr groben - Kennzeichnung ausreicht: Befindet sich das einer festgelegten Position nächstgelegene Merkmal in der definierten Richtung bezüglich dieser

Position, so wird beispielsweise eine "1" gegeben, ansonsten eine "0". Durch Benutzung mehrwertiger Symbole ist eine Zuordnung zu mehreren Positionen/Abständen bzw. Richtungen möglich, was in einer gewissen Analogie zu einer n-QPSK-Modulation in der Nachrichtentechnik steht.

Auch die Richtung eines Merkmals (beispielsweise einer Verzweigung oder eines Linienendes eines Papillarlinienmusters) kann im einfachsten Fall durch ein Bit ausgedrückt werden, beispielsweise durch eine "0" für ein nach oben gerichtetes Merkmal und eine "1" für ein nach hinten gerichtetes. (Natürlich müssen auch Daten bezüglich der Referenzposition(en) bzw. -richtung(en) mitgeführt werden.)

Wie auch bei der Kennzeichnung der Positionen, ist durch mehrwertige Symbole auch eine feinere Richtungs-Unterscheidung möglich, beispielsweise mit zwei Bit die Unterscheidung von vier Richtungen, was in gewisser Analogie zu einer n-PSK-Modulation in der Übertragungstechnik steht. Grundsätzlich liegt es im Rahmen der Erfindung, die numerische (binäre) Repräsentation der Merkmalslage und -richtung mit einer relativ groben Auflösung durchzuführen, die zu einer hinreichend zuverlässigen Authentifikation aufgrund biometrischer Merkmalskomplexe gerade ausreicht. Dies reduziert den Speicherplatzbedarf und die benötigte Auswertungszeit.

Der auf diese oder ähnliche Weise beispielsweise unter Nutzung eines Koordinatenrasters (siehe dazu weiter unten) ausgedrückten Lage- und/oder Richtungsinformation wird noch eine Kennzeichnung des Merkmalstyps bzw. der Merkmalsklasse hinzugefügt. Diese kann beispielsweise in einer Binärdarstellung der für die verschiedenen Merkmalstypen in Fig. 1 benutzten Bezugsziffer bestehen. Werden in einer vereinfachten Ausführung beispielsweise nur Linienverzweigungen und Linienenden herangezogen, so reicht ein Bit (1 oder 0) zur Kennzeichnung des Merkmalstyps aus.

- In Fig. 3 ist skizziert, wie der Gesamtfläche eines Fingerabdrucks gemäß Fig. 1 (gestrichelt umrandet) ein Koordinatenraster hinterlegt wird, um eine hinreichend genaue Lage- und Richtungsdarstellung ausgewählter Merkmale vornehmen zu können. In dieser Figur sind Linienverzweigungen in Form eines "Y" und Linienenden als offene Kreise symbolisiert; die binäre Darstellung wäre beispielsweise - wie oben bereits erwähnt - "1" oder "0". Im Beispiel gemäß der Figur hat das Koordinatenraster $6 \times 9 = 54$ Bezugfelder, so daß die Lagekennzeichnung eines Merkmals mit 7 Bit möglich ist. Zweckmäßigerweise wird die Richtung der Verzweigungspunkte (Merkmaltyp "1") mit zwei zusätzlichen Bit (nach oben, unten, rechts oder links orientiert) ausgedrückt, so daß jede Element-Binärzahl zehnstellig ist. Im Beispiel ist die Anzahl der ausgewerteten Merkmalselements 31, so daß das Papillarliniemuster insgesamt durch ein n-Tupel mit $n = 31$ und (idealisiert) insgesamt 310 Bit Wortlänge darstellbar ist. Dies ist allerdings bereits eine sehr detaillierte Darstellung, und im Normalfall wird für die Erzeugung einer PIN für die Zugangskontrolle zu einem Mobilfunknetz die Auswertung einer geringeren Anzahl von Merkmalen mit einem gröberen Koordinatenraster ausreichend sein, was zu einem entsprechend verringerten Umfang der binären Darstellung führt.
- Wie oben bereits erwähnt, wird zur Gewinnung einer PIN die den Merkmalskomplex repräsentierende Bitsequenz einer bekannten redundanten bzw. fehlerkorrigierenden Codierung nach dem Reed-Solomon- oder einem anderen bekannten Verfahren unterzogen. Die auf diese Weise erhaltene PIN dient als Vergleichsbasis gegenüber einer auf der SIM-Karte gespeicherten PIN beim eigentlichen Authentifikationsvorgang.

Fig. 4 zeigt skizzenhaft die im Zusammenhang mit der Erläuterung einer Ausführungsform der Erfindung wesentlichen Funktionskomponenten einer Vorrichtung zur Nutzer-Authentifikation bei einem Mobiltelefon 10 mit einer SIM-Karte 20. In einem PIN-Speicherbereich 21 der SIM-Karte ist die dem auto-

risierten Nutzer zugewiesene PIN gespeichert. Das Mobiltelefon 10 weist einen einer Fingermulde 11a zugeordneten CCD-Sensorbaustein zur bildmäßigen Erfassung des Papillarlinienmusters der Fingerkuppe eines Nutzers auf, dem eine Bildverarbeitungsstufe 12 nachgeordnet ist. Deren Ausgang ist mit einer Merkmals-Extraktionsstufe 13 verbunden, der ein Merkmalscodierer 14 nachgeschaltet ist. Dessen Ausgang ist mit einer PIN-Berechnungsstufe 15 verbunden, die auf einen nichtflüchtigen Algorithmenspeicher 16 zugreift und deren Ausgang mit einem Eingang einer hier (gemäß GSM-Protokoll) wiederum auf der SIM-Karte realisieren PIN-Vergleichereinheit 17 verbunden ist, deren anderer Eingang mit dem PIN-Speicherbereich 21 der SIM-Karte verbunden ist. Am Ausgang der PIN-Vergleichereinheit 17 steht ein durch den Vergleich der vorgespeicherten PIN mit einer aus dem Papillarlinienmuster aufgrund eines vorgespeicherten Algorithmus berechneten PIN gewonnenes Authentifikationssignal bereit, mit dem - bei Übereinstimmung - ein Netzzugang und/oder Zugang zu auf der SIM-Karte gespeicherten Daten bzw. - bei Nichtübereinstimmung - dessen Verweigerung gesteuert wird.

Die Ausführung der Erfindung ist nicht auf die beschriebenen Ausführungsformen beschränkt, sondern auch in einer Vielzahl von Abwandlungen möglich. So stellt ein Mobiltelefon nur einen von vielen Anwendungsbereichen dar; weitere sind die Computer-, Datenbank-, Datendienst- oder Medien-Zugangskontrolle. Die Vorteile der vorgeschlagenen Lösung ermöglichen deren Einsatz auch im Privatbereich, beispielsweise bei der Zugangskontrolle für Fernsehgeräte oder Internet-Dienste. Die Zuordnung des Kennzeichnungsspeichers und der Vergleichermittel kann, speziell in Systemen unter Einsatz weniger "intelligenter" Chipkarten, auch - statt einer Realisierung auf der Chipkarte - zum eigentlichen Gerät oder zum Netz, d.h. zu einer zentralen Datenbank o.ä., erfolgen.

Patentansprüche

1. Verfahren zur Nutzer-Authentifikation beim Zugang zu einem Objekt, System oder Dienst aufgrund eines als Flächenmuster
5 erfaßten biometrischen Merkmalskomplexes, wobei aus dem Flächenmuster eine Mehrzahl von charakteristischen Merkmalselementen extrahiert wird,
dadurch gekennzeichnet,
daß quantisierte Lage- und/oder Richtungsbeziehungen der
10 Merkmalselemente zueinander und/oder zu vorbestimmten Bezugspunkten bzw. -richtungen ermittelt werden und im Ergebnis jedem Merkmalselement eine Element-Zahl, insbesondere Element-Binärzahl, zugeschrieben wird und mittels eines vorbestimmten Codierungsalgorithmus aus den Element-Zahlen eine
15 numerische oder alphanumerische Identifikations-Kennzeichnung berechnet sowie diese mit einer vorgespeicherten Identifikations-Kennzeichnung verglichen wird.
2. Verfahren nach Anspruch 1,
20 dadurch gekennzeichnet,
daß als charakteristische Merkmalselemente ausgewählte Linienenden (6) und/oder -verzweigungen (2) eines in dem Flächenmuster enthaltenen Linienmusters extrahiert werden und in die Element-Zahl jeweils eine Lage- und eine auf den Linien-
25 verlauf bezogene Richtungsinformation, bezogen auf eine Referenzrichtung, einbezogen wird.
3. Verfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
30 daß zur Berechnung der Identifikations-Kennzeichnung aus den Element-Zahlen ein fehlerkorrigierender Codierungsalgorithmus angewandt wird.
4. Verfahren nach einem der vorangehenden Ansprüche,
35 dadurch gekennzeichnet,
daß in die Bildung der Element-Zahlen eine Fehlergrenz-Information einbezogen wird, die die Wahrscheinlichkeit des

Zutreffens der in der jeweiligen Element-Zahl ausgedrückten Lage- und/oder Richtungsbeziehung in Abhängigkeit von der Auflösung der vorbestimmten Bezugspunkte bzw. -richtungen quantifiziert.

5

5. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet,

10 daß aus den extrahierten charakteristischen Merkmalen eines Teilbereichs des Flächenmusters oder anhand einer Teilmenge der extrahierten Merkmalselemente eine Positions- und Lagekorrekturinformation, insbesondere in Form einer Transformations-Binärzahl abgeleitet wird, die im Schritt der Ermittlung quantisierter Lage- und/oder Richtungsbeziehungen angewandt wird.

15

6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet,

20 daß eine vorbestimmte Menge von Codierungsalgorithmen vorgesehen ist, von denen einer durch den Nutzer ausgewählt werden kann.

7. Verfahren nach einem der vorangehenden Ansprüche, gekennzeichnet durch

25 die Anwendung bei einem Mobilfunk-Endgerät (10) bei jedem Einschalten und/oder vor jedem Verbindungsaufbau.

8. Vorrichtung zur Durchführung des Verfahrens nach einem der vorangehenden Ansprüche, mit

30 einer Flächenmuster-Erfassungseinrichtung (11), einer der Flächenmuster-Erfassungseinrichtung mindestens mittelbar nachgeordneten Merkmals-Extraktionseinrichtung (13), einem der Merkmals-Extraktionseinrichtung nachgeordneten binären Merkmalscodierer (14) zur Bildung von Element-Binärworten für jedes der in der Merkmals-Extraktionseinrichtung
35 extrahierten charakteristischen Merkmale, einer Identifikationskennzeichnungs-Berechnungsstufe (15) zur Berechnung einer Identifikations-Kennzeichnung aus den Ele-

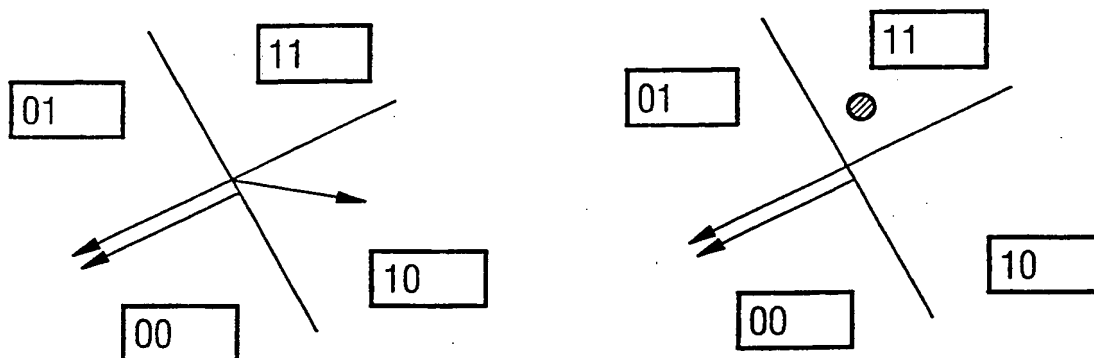
- ment-Binärworten aufgrund eines in einem Algorithmenspeicher (16) gespeicherten, insbesondere fehlerkorrigierenden, Berechnungsalgorithmus, und einer Identifikationskennzeichnungs-Vergleichereinheit (17) zum Vergleich der aus dem Flächenmuster abgeleiteten Identifikations-Kennzeichnung mit einer vorgespeicherten Identifikations-Kennzeichnung und zur Ausgabe eines das Vergleichsergebnis widerspiegelnden Authentifikationssignals.
- 10 9. Mobiltelefon (10) mit einer Vorrichtung (11 bis 17) nach Anspruch 8, dadurch gekennzeichnet, daß auf einer SIM-Karte (20) ein Identifikations-Kennzeichnungs-Speicher (21) vorgesehen ist, der ausgangsseitig mit
- 15 der Identifikations-Kennzeichnungs-Vergleichereinheit (17) verbunden ist.

1/3

FIG 1



FIG 2



2/3

FIG 3

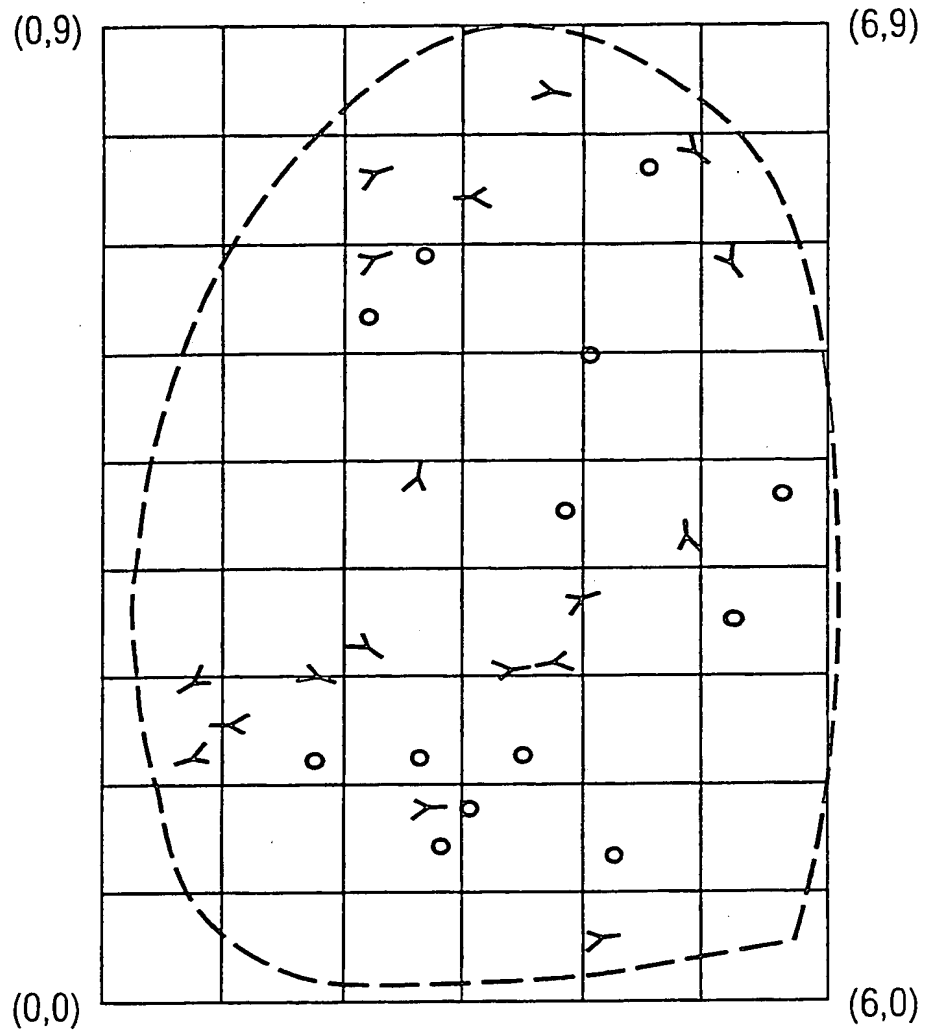
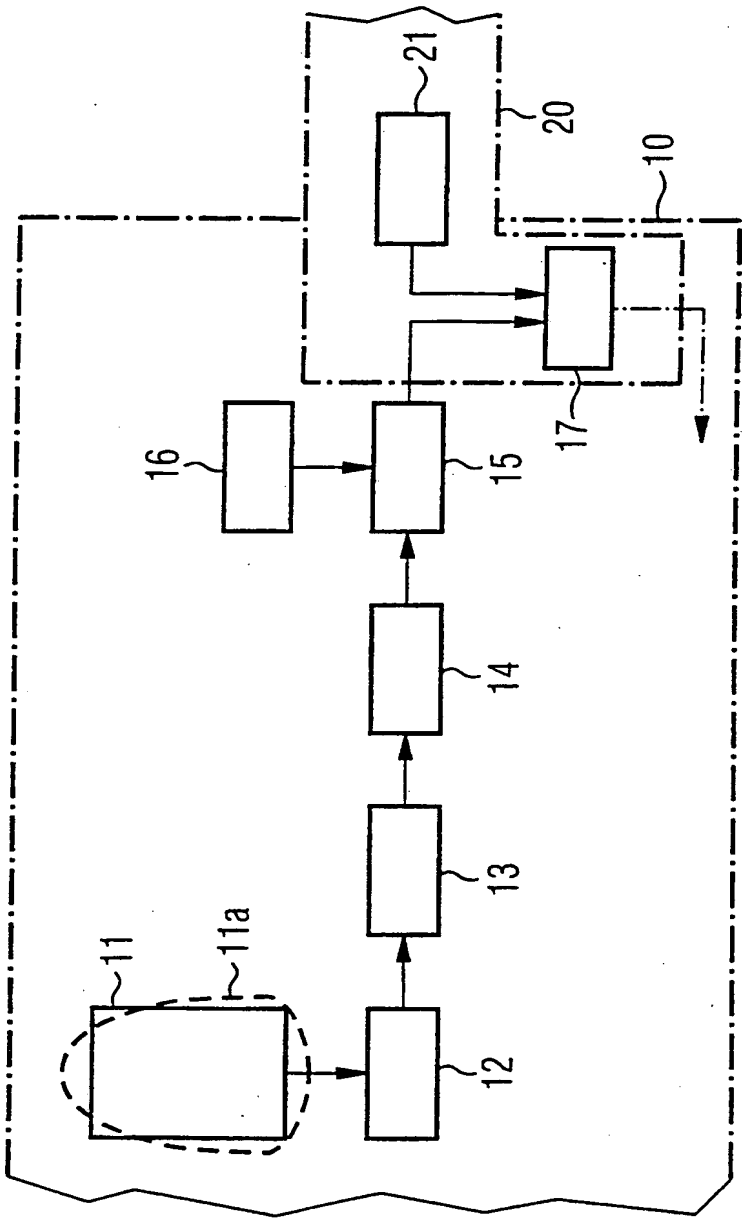


FIG 4



INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 00/01020

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K9/46 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4 325 570 A (ESTRADA CARLOS I) 20 April 1982 (1982-04-20) the whole document	1,8
A	US 5 598 474 A (NELDON P JOHNSON) 28 January 1997 (1997-01-28) column 11, line 50 -column 12, line 31	1,8
A	US 4 995 086 A (LILLEY ROBERT M ET AL) 19 February 1991 (1991-02-19) column 3, line 15 - line 58	1,8
A	FR 2 582 831 A (RAVEL ROGER) 5 December 1986 (1986-12-05) page 15, line 3 -page 16, line 4	1,8
	-/-	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

15 August 2000

Date of mailing of the international search report

21/08/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Sonius, M

INTERNATIONAL SEARCH REPORT

Inte .onal Application No
PCT/DE 00/01020

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 33 35 678 A (SIEMENS AG) 18 April 1985 (1985-04-18) page 8, line 4 - line 10 <u> </u>	1,8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE 00/01020

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 4325570	A	20-04-1982	NONE	
US 5598474	A	28-01-1997	AU 693655 B AU 4805096 A BR 9600961 A CN 1137659 A EP 0731426 A JP 9114986 A	02-07-1998 19-09-1996 30-12-1997 11-12-1996 11-09-1996 02-05-1997
US 4995086	A	19-02-1991	EP 0244498 A AT 64484 T DE 3679819 D JP 62278685 A	11-11-1987 15-06-1991 18-07-1991 03-12-1987
FR 2582831	A	05-12-1986	NONE	
DE 3335678	A	18-04-1985	NONE	

INTERNATIONALER RECHERCHENBERICHT

Inte lionales Aktenzeichen

PCT/DE 00/01020

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06K9/46 G07C9/00

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06K G07C

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 4 325 570 A (ESTRADA CARLOS I) 20. April 1982 (1982-04-20) das ganze Dokument	1,8
A	US 5 598 474 A (NELDON P JOHNSON) 28. Januar 1997 (1997-01-28) Spalte 11, Zeile 50 -Spalte 12, Zeile 31	1,8
A	US 4 995 086 A (LILLEY ROBERT M ET AL) 19. Februar 1991 (1991-02-19) Spalte 3, Zeile 15 - Zeile 58	1,8
A	FR 2 582 831 A (RAVEL ROGER) 5. Dezember 1986 (1986-12-05) Seite 15, Zeile 3 -Seite 16, Zeile 4 -/-	1,8

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

15. August 2000

Abmeldedatum des internationalen Recherchenberichts

21/08/2000

Name und Postanschrift der internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Sonius, M

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/DE 00/01020

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 33 35 678 A (SIEMENS AG) 18. April 1985 (1985-04-18) Seite 8, Zeile 4 - Zeile 10	1,8

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/DE 00/01020

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
US 4325570	A	20-04-1982	KEINE		
US 5598474	A	28-01-1997	AU	693655 B	02-07-1998
			AU	4805096 A	19-09-1996
			BR	9600961 A	30-12-1997
			CN	1137659 A	11-12-1996
			EP	0731426 A	11-09-1996
			JP	9114986 A	02-05-1997
US 4995086	A	19-02-1991	EP	0244498 A	11-11-1987
			AT	64484 T	15-06-1991
			DE	3679819 D	18-07-1991
			JP	62278685 A	03-12-1987
FR 2582831	A	05-12-1986	KEINE		
DE 3335678	A	18-04-1985	KEINE		